TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 1421	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 03/03681	Date du dépôt international *(jour/mois/année)* 11/12/2003	(Date de priorité (la plus ancienne) *(jour/mois/année)* 11/12/2002
Déposant GEMPLUS		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[ ] le texte est approuvé tel qu'il a été remis par le déposant

[X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

[ ] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR 03/03681

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

ABREGE

L'invention concerne un procédé cryptographique au cours duquel on realisé une division entière de type q = a div b et / ou une réduction modulaire de type r = a mod b, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort du nombre b.

Selon l'invention, on masque le nombre a par un nombre aléatoire p avant de réaliser la division entière et / ou la réduction modulaire.

L'invention concerne également un composant électronique pour la mise en oeuvre du procédé ci-dessus.

Application à la sécurisation des cartes à puce contre les attaques à canaux cachés, et notamment les attaques différentielles.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/03681

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	DE 199 63 407 A (GIESECKE & DEVRIENT GMBH) 12 juillet 2001 (2001-07-12) colonne 1, ligne 42 -colonne 3, ligne 53 ---	1-8
A	EP 0 682 327 A (YEDA RES & DEV) 15 novembre 1995 (1995-11-15) le document en entier -----	1-8

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
27 avril 2004	- 5. MAI 2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/03681

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 19963407 A	12-07-2001	DE 19963407 A1	12-07-2001
		AU 3015101 A	09-07-2001
		CN 1415106 T	30-04-2003
		WO 0148706 A1	05-07-2001
		EP 1272984 A1	08-01-2003
		JP 2003525538 T	26-08-2003
		US 2003079139 A1	24-04-2003
EP 0682327 A	15-11-1995	US 5504817 A	02-04-1996
		EP 0682327 A2	15-11-1995
		IL 113662 A	06-12-2000